REMARKS

In the Official Action mailed on **2 June 2006**, the Examiner reviewed claims 1-11, 13-29, 31-47, and 49-54. Claims 1, 4, 5, 8, 9, 13, 15, 16, 18, 19, 22, 23, 26, 27, 31, 33, 34, 36, 37, 40, 41, 44, 45, 49, 51, 52, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier (*Applied Cryptography 2nd Edition*, Oct. 1995, John Wiley & Sons Pub. pages 43-57, hereinafter "Schneier") in view of Medvinski et al (*Public Key Utilizing Tickets for Application Servers*, hereinafter "Medvinski") and Kohl et al (*The Kerberos Network Authentication Service, Network Working Group Request For Comments (RFC)* 1510, Sept. 1993, hereinafter "Kohl"). Claims 14, 17, 32, 35, 50, and 53 were rejected as being unpatentable over Schneier in view of Medvinski and Official Notice (hereinafter "ON"). Claims 2, 3, 6, 7, 10, 11, 20, 21, 24, 25, 28, 29, 38, 39, 42, 43, 46, and 47 were rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Medvinski and Sirbu et al (*Public Key Based Ticket Granting service in Kerberos*, hereinafter "Sirbu") and ON.

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 19, and 37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Medvinski and Kohl.

Examiner avers in both the instant office action and the previous office action, that "Medvinski teaches the use of a secret key with a limited lifespan intended to reduce KDC vulnerability on page 57: 'Key Expiration'."

Unfortunately, Applicant failed to find the reference "Medvinski, page 57: 'Key Expiration'" during the procedure of previous office action response. Applicant has communicated with Examiner in an attempt to obtain aforementioned reference. However, so far the reference has not been provided.

Applicant respectfully points out that the session key with a limited lifespan taught by Schneier on page 47, Sec. 3.1 "Key Exchange" is the same type of session key taught by Kohl in Kerberos. These session keys are used for only

one communication session, thereby having a limited lifespan. Hence, Applicant acknowledges that the session key and the temporary secret key of the instant application are both communication keys with limited lifespan.

However, the temporary secret key of the instant application is different from a session key in the following aspects: the temporary secret key, after being created, is **stored in a database** at the KDC, so that the temporary secret key can be used to facilitate **one or more communications** between two communicants **at a later time** (see page 11, lines 5-9). In contrast, the session key is generated at the time that two principals (e.g., a client and a server) need to establish a communication, and then shared by the two principals during the specific communication session. Hence, **the session key is not stored in a database for later use**, and is used for only **one** communication session before being discarded. Note that the main motivation behind using the temporary secret to replace a long-term one is that if an adversary could obtain access to the database storing such secret keys, he/she would be able to access all of the long-term secrets stored there. In contrast, a session key does not suffer from this vulnerability because it is not stored in a database during its limited lifespan.

Accordingly, Applicant has amended independent claims 1, 19, and 37 to clarify that the temporary secret key of the instant application is stored in a database at the KDC, so that the temporary secret key can be used to facilitate one or more communications between two communicants at a later time. These amendments find support on page 9, lines 11-17, and page 11, lines 5-9 of the instant application.
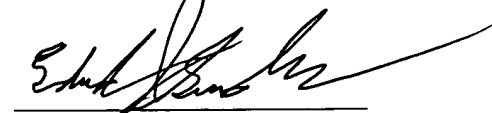
Hence, Applicant respectfully submits that independent claims 1, 19, and 37 as presently amended are in condition for allowance. Applicant also submits that claims 2-11 and 13-18, which depend upon claim 1, claims 21-29 and 31-36, which depend upon claim 19, and claims 38-47 and 49-54, which depend upon claim 37, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By

Edward J. Grundler
Registration No. 47,615

Date: 1 September 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com